

# PATENT ABSTRACTS OF JAPAN

(11) Publication number : 2002-207649  
 (43) Date of publication of application : 26.07.2002

) Int. CI.

G06F 13/00  
 H04M 3/00

) Application number : 2001-000060

(71) Applicant : NEC CORP  
 NTT COMMUNICATIONS KK

) Date of filing : 04.01.2001

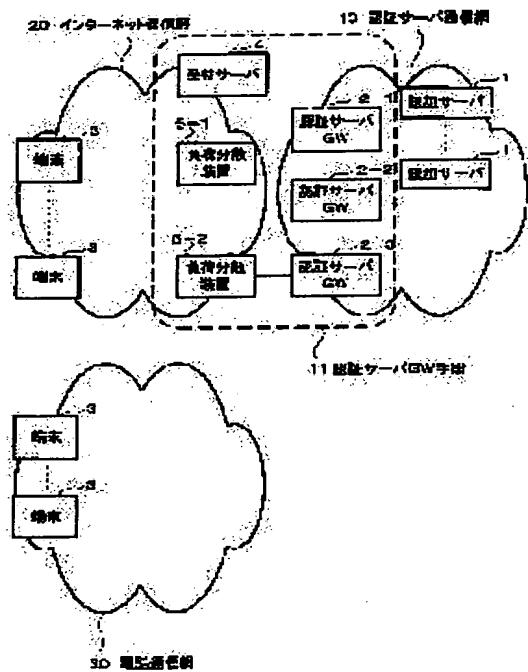
(72) Inventor : FUJINAMI MASAO  
 INOUE TAKUYA  
 MIZOGUCHI YOICHI

## I) INTERNET LOAD-DECENTRALIZED RELAYING CONNECTION SYSTEM

### I) Abstract:

PROBLEM TO BE SOLVED: To decentralize the load on a plurality of authentication service GW devices and to make a large number of sec connections from dial-up terminals.

SOLUTION: Multiple authentication server GW devices which terminate IPsec are installed, a load decentralizing device which administers the authentication server GW devices (monitors their life/death states is placed), and a reception server is provided so that authentication server GWs are seen from a terminal side as if there were one authenticating server GW. The reception server monitors the life/dead state and use state (number of connections) of the load distributing device to send an address of an authentication server GW back to the terminal.



### EXAMINER'S STATUS

Date of request for examination] 01.02.2002

Date of sending the examiner's decision of rejection]

Date of final disposal of application other than the examiner's decision of rejection or application converted registration]

Date of final disposal for application]

Patent number]

Date of registration]

umber of appeal against examiner's decision of  
jection]

ate of requesting appeal against examiner's  
cision of rejection]

ate of extinction of right]

Copyright (C) ; 1998, 2003 Japan Patent Office

(19) 日本国特許庁 (JP)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号

特開 2002-207649

(P 2002-207649 A)

(43) 公開日 平成14年7月26日 (2002.7.26)

(51) Int. C1.<sup>7</sup>  
 G 06 F 13/00  
 H 04 M 3/00

識別記号  
 357

F I  
 G 06 F 13/00 357 Z 5B089  
 H 04 M 3/00 B 5K051

審査請求 有 請求項の数 6 O L (全 7 頁)

(21) 出願番号 特願2001-60 (P2001-60)

(22) 出願日 平成13年1月4日 (2001.1.4)

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(71) 出願人 399035766

エヌ・ティ・ティ・コミュニケーションズ  
株式会社

東京都千代田区内幸町一丁目1番6号

(72) 発明者 藤波 正雄

東京都港区芝五丁目7番1号 日本電気株式  
会社内

(74) 代理人 100078237

弁理士 井出 直孝 (外1名)

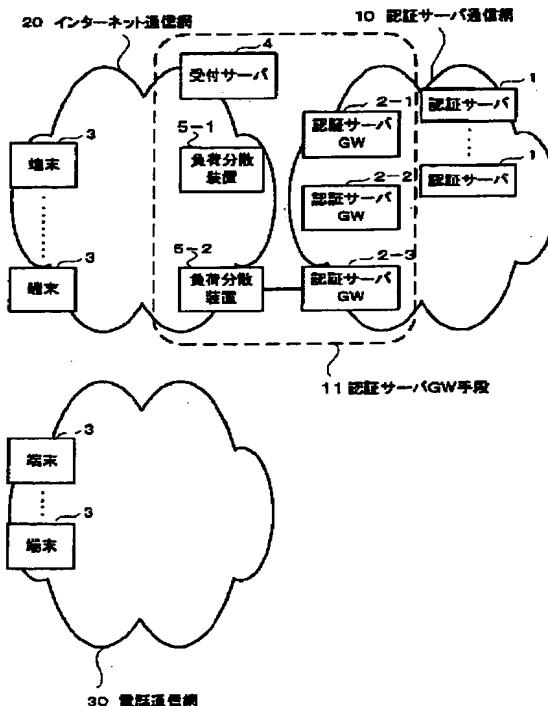
最終頁に続く

(54) 【発明の名称】 インターネット負荷分散中継接続方式

## (57) 【要約】

【課題】 複数の認証サービスGW装置に対する負荷分散を可能にするとともに、ダイアルアップ端末からの膨大な数のIPsecコネクション確立を可能とする。

【解決手段】 IPsecを終端する認証サーバGW装置を複数台設置し、さらに認証サーバGW装置を取りまとめる（生死状態を監視する）負荷分散装置を置き、さらに、端末側から認証サーバGWが一つに見えるように受付サーバを置く。受付サーバは負荷分散装置の生死状態と使用状況（接続数）を監視することによって、認証サーバGWのアドレスを端末に返送する。



## 【特許請求の範囲】

【請求項1】 複数の認証サーバを含みインターネット・プロトコル（IP, internet protocol）に準拠するIPアドレスにより制御される認証サーバ通信網（CSN, certified server network）とインターネット通信網との接続点に設けられた認証サーバGW（gate way）手段を備え、

この認証サーバGW手段は、インターネット・プロトコルに準拠するアドレスが付与される多数の端末からインターネット通信網を介してアクセス可能なインターネット負荷分散中継接続方式において、

前記認証サーバGW手段は、前記インターネット通信網側からは一つの認証サーバGWとして認識される受付サーバと、複数の認証サーバGW装置と、それぞれ前記受付サーバに接続され前記複数の認証サーバGW装置をグループ毎に統括制御する一つまたは複数の負荷分散装置とを含むことを特徴とするインターネット負荷分散中継接続方式。

【請求項2】 前記端末は、電話通信網内にあり、ダイアルアップによりインターネット・プロトコルに準拠するアドレスがその接続の都度付与され、その接続状態が終了したときにはそのアドレスが削除されるアドレス非固定端末を含む請求項1記載のインターネット負荷分散中継接続方式。

【請求項3】 前記受付サーバは、配下の負荷分散装置の動作状態および接続数を管理する手段と、この管理する手段により接続可能な負荷分散装置およびそのアドレスを認識する手段とを含む請求項2記載のインターネット負荷分散中継接続方式。

【請求項4】 前記受付サーバは、前記端末からの問い合わせに対して接続可能な負荷分散装置のアドレスをその端末に対して回答する手段を含む請求項3記載のインターネット負荷分散中継接続方式。

【請求項5】 前記負荷分散装置は、その配下の認証サーバGW装置の動作状態および接続数を管理する手段と、この管理する手段により接続可能な認証サーバGW装置およびそのアドレスを認識する手段と、この手段により認識された接続可能な認証サーバGW装置のアドレスを前記端末に提供する手段とを含む請求項4記載のインターネット負荷分散中継接続方式。

【請求項6】 前記端末は、前記受付サーバからの問い合わせ応答に対応して動作中の認証サーバGW装置に対してインターネット・プロトコルによるセキュリティ接続（IPsec）を確立する手段を含む請求項2記載のインターネット負荷分散中継接続方式。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、インターネット通信網から正当な端末であることの認証を受けるために、認証サーバにアクセスする中継接続に利用する。本発明

は、ダイアルアップ端末などインターネット・プロトコル（IP）アドレスが固定的に設定されていない端末から、インターネット・プロトコルにより認証サーバにアクセスするための中継接続に関する。本発明は、きわめて多数の端末が認証サーバにアクセスすることを許容する中継接続に利用する。本発明は認証サーバの負荷分散に関する。

## 【0002】

【従来の技術】 ユーザがネットワークを介して目的のサービス提供者のサーバに接続し、そのサーバから情報提供その他のサービスを受けるときに、当該サービス提供者のサーバは、サービス提供を求めてきたユーザの正当性を認証し、認証が得られた端末に対して相応のサービスを提供するための技術が知られている。サービス提供者側では、この認証の種類および数に対応して、一つのネットワークの中に認証処理を行う認証サーバを複数設置することが行われている。

【0003】 このような認証処理を行うには、ユーザと認証サーバとの間に、インターネット・プロトコル（IP）によるセキュリティ接続（IPsecコネクション）を確立して、他の端末または他の接続から通信内容を盗用されることがないように通信を行う必要がある。また、このようなサービスを求める端末には、固定的なIPアドレスが付与されていない端末、たとえば電話通信網からダイアルアップにより接続を求めるIPアドレス非固定端末も含まれる。この場合には、きわめて大量な接続を一時に処理しなければならない場合がしばしば発生する。

## 【0004】

【発明が解決しようとする課題】 このような従来の認証サービスの課題は、大量の認証要求が発生しているときに、配置されている複数の認証サーバGW装置のうち、どの認証サーバGW装置とIPsecコネクションを確立することが、負荷分散のために合理的であるか判断がつかないことである。すなわち従来方式では、各認証サーバGW装置の稼働または非稼働の状態（生死状態という）は接続制御側で認識できるようになっていない。また各認証サーバGW装置について、それぞれ現時点の接続可能な数が認識できるように構成されていない。したがって、一つの認証サーバに集中的に接続要求が行われる、接続可能な数がきわめて小さい認証サーバに接続可能な数を越える接続要求が行われるなどの状況が発生し、これらの接続要求は接続失敗となり接続要求中の端末が増大することになる。

【0005】 本発明は、このような背景に行われたものであって、複数の認証サーバGW装置の負荷分散を合理的に行うとともに、接続失敗の可能性を小さくすることができるインターネット負荷分散中継接続方式を提供することを目的とする。

## 【0006】

【課題を解決するための手段】本発明は、膨大な数のIPsecコネクションに対して、IPsecを終端する認証サーバGW装置を複数台設置し、さらに複数の認証サーバGW装置を取りまとめ、その生死状態を監視することができる負荷分散装置を置き、さらに、端末側から認証サーバが一つに見えるように受付サーバを置く。そして、受付サーバにより負荷分散装置の生死状態と使用状況（接続数）を監視し、接続可能な認証サーバGW装置のアドレスを接続要求を行う端末に返送する。

【0007】これにより、複数の負荷分散装置を受付サーバが管理し、端末から受付サーバに接続可能な認証サーバGW装置のアドレスを問合せができる。受付サーバは、端末からの問合せに対し、認証サーバGW装置のアドレスを回答する。また、認証サーバGW装置の前段に負荷分散装置があるから、端末側には複数の認証サーバGW装置を一台に見せることができる。さらに、受付サーバが認証サーバGW装置の生死状態と使用状況（接続数）を取得して管理し、受付サーバが取得した生死状態と使用状況（接続数）より認証サーバGW装置のアドレスを求める、あるいは、負荷分散装置が認証サーバGW装置の生死状態を認識することもできる。動作中の認証サーバGW装置に対しIPsecコネクションを確立することもできる。

【0008】すなわち、本発明は、複数の認証サーバ（1）を含みインターネット・プロトコル（IP, internet protocol）に準拠するIPアドレスにより制御される認証サーバ通信網（CSN, certified server network）（10）とインターネット通信網（20）との接続点に設けられた認証サーバGW（gate way）手段（11）を備え、この認証サーバGW手段（11）は、インターネット・プロトコルに準拠する非固定的なアドレスが付与される多数の端末（3）からインターネット通信網（20）を介してアクセスされるように設定されたインターネット負荷分散中継接続方式であり、本発明の特徴とするところは、前記認証サーバGW手段（11）は、前記インターネット通信網側からは一つの認証サーバGWとして認識される受付サーバ（4）と、それぞれ前記受付サーバに接続され前記複数の認証サーバGW装置をグループ毎に統括制御する一つまたは複数の負荷分散装置（5）とを含むところにある。

【0009】上記括弧内の数字は後から説明する実施例の図面符号である。これは本発明の構成を理解しやすいように付したものであって、本発明を実施例に限定して理解するためのものではない（以下同じ）。

【0010】前記端末は、電話通信網（30）内にあり、ダイアルアップによりインターネット・プロトコルに準拠するアドレスがその接続の都度付与され、その接続状態が終了したときにはそのアドレスが削除される端末を含む構成とする場合にも対応することができる。

【0011】前記受付サーバ（4）は、配下の負荷分散

装置（5）の動作状態および接続数を管理する手段と、この管理する手段により接続可能な負荷分散装置およびそのアドレスを認識する手段とを含む構成とすることもできる。

【0012】前記受付サーバ（4）は、前記端末からの問い合わせに対して接続可能な負荷分散装置のアドレスをその端末に対して回答する手段を含む構成とすることもできる。

【0013】前記負荷分散装置（5）は、その配下の認

証サーバGW装置の動作状態および接続数を管理する手段と、この管理する手段により接続可能な認証サーバGW装置およびそのアドレスを認識する手段と、この手段により認識された接続可能な認証サーバGW装置のアドレスを前記端末に提供する手段とを含む構成とすることもできる。

【0014】前記端末（3）は、前記受付サーバからの問い合わせ応答に対応して動作中の認証サーバGW装置に対してインターネット・プロトコルによるセキュリティ接続（IPsec）を確立する手段を含む構成とすることもできる。

【0015】

【発明の実施の形態】本発明実施例のインターネット負荷分散中継接続方式の構成を図1を参照して説明する。図1は本発明実施例のインターネット負荷分散中継接続方式の全体構成図である。

【0016】本発明は、図1に示すように、複数の認証サーバ1を含みインターネット・プロトコルに準拠するIPアドレスにより制御される認証サーバ通信網10とインターネット通信網20との接続点に設けられた認証サーバGW装置2-1～2-3を備え、この認証サーバGW装置2-1～2-3は、インターネット・プロトコルに準拠する非固定的なアドレスが付与される多数の端末3からインターネット通信網20を介してアクセスされるように設定されたインターネット負荷分散中継接続方式である。

【0017】ここで、本発明の特徴とするところは、複数の認証サーバGW装置2-1～2-3は、インターネット通信網20側からは一つの認証サーバGW手段11として認識されるように構成されたところにある。すなわち、認証サーバGW手段11は、一つの受付サーバ4と、それぞれ受付サーバ4に接続され複数の認証サーバGW装置2-1～2-3をグループ毎に統括制御する一つまたは複数の負荷分散装置5-1、5-2とを含むように構成される。

【0018】電話通信網30内の端末3については、ダイアルアップによりインターネット・プロトコルに準拠するアドレスがその接続の都度付与され、その接続状態が終了したときにはそのアドレスが削除される。

【0019】受付サーバ4は、配下の負荷分散装置5-1および5-2の動作状態および接続数を管理し、接続

可能な負荷分散装置 5-i (i は 1、2 のいずれか) およびそのアドレスを認識する。

【0020】受付サーバ 4 は、端末 3 からの問い合わせに対して接続可能な負荷分散装置 5-i のアドレスをその端末 3 に対して回答する。

【0021】負荷分散装置 5-1、5-2 は、その配下の認証サーバ GW 装置 2-1～2-3 の動作状態および接続数を管理し、接続可能な認証サーバ GW 装置 2-j (j は 1、2、3 のいずれか) およびそのアドレスを認識し、認識された接続可能な認証サーバ GW 装置 2-j のアドレスを端末 3 に提供する。

【0022】端末 3 は、受付サーバ 4 からの問い合わせ応答に対応して動作中の認証サーバ GW 装置 2-1～2-3 に対してインターネット・プロトコルによるセキュリティ接続 (IPsec) を確立する。

【0023】このように、本発明実施例のインターネット負荷分散中継接続方式は、膨大な IPsec を確立するために、認証サーバ GW 装置 2-1～2-3 および負荷分散装置 5-1、5-2 を複数台備え、IP ネットワークであるインターネット通信網 20 は、端末 3、受付サーバ 4、負荷分散装置 5-1、負荷分散装置 5-2 で構成される。IP ネットワークである認証サーバ通信網 10 は、認証サーバ GW 装置 2-1、認証サーバ GW 装置 2-2、認証サーバ GW 装置 2-3 および認証サーバ群で構成される。

【0024】以下に本発明実施例をさらに詳細に説明する。

【0025】図 1において、受付サーバ 4 は負荷分散装置 5-1、負荷分散装置 5-2 を管理しており、それぞれの生死状態と使用状況（接続数）を取得し管理している。また、負荷分散装置 5-1 は認証サーバ GW 装置 2-1、認証サーバ GW 装置 2-2 の生死状態を負荷分散装置 5-2 は認証サーバ GW 装置 2-3 の生死状態を認識している。

【0026】端末 3 がダイアルアップして任意のアドレスを付与され、複数の認証サーバ GW 装置 2 と IPsec コネクションを確立する際に、まず、受付サーバ 4 に認証サーバ GW アドレスを問合せる。受付サーバ 4 では、生死状態と使用状況（接続数）により負荷分散装置 5 のアドレス IP:3 を求め応答する。端末 3 では得られた負荷分散装置 5 のアドレス IP:3 を使用して IPsec 接続要求（認証）を行うと、負荷分散装置 5 が生死状態を認識し、動作中の認証サーバ GW 装置 2-2 に対し振分ける。認証サーバ GW 装置 2-2 にて IPsec 認証を行い、許容であれば IPsec 接続応答（認証）を返送する。

【0027】このようにして、本発明では、ダイアルアップした端末 3 から複数の認証サービス GW 装置 2-1～2-3 を 1 台に見せ、動作中の認証サーバ GW 装置 2-i に対して IPsec コネクションを確立することが

できる。

【0028】次に、本発明実施例のインターネット負荷分散中継接続方式の動作を図 2 を参照して詳しく説明する。図 2 は本発明実施例のインターネット負荷分散中継接続方式の動作を示すシーケンス図である。受付サーバ 4 は管理している負荷分散装置 5-1 および 5-2 に対し定期的に生死状態および使用状況（接続数）を取得する。また、負荷分散装置 5-1 では認証サーバ GW 装置 2-1 および 2-2 を監視し、生死状態を認識している。同様に負荷分散装置 5-2 では認証サーバ GW 装置 2-3 を監視し、生死状態を認識している。

【0029】端末 3 がダイアルアップし、認証サーバ群と IPsec コネクションを使用して通信するためには負荷分散装置 5-1、5-2 および認証サーバ GW 装置 2-1～2-3 を経由する必要がある。負荷分散装置 5-1、5-2 および認証サーバ GW 装置 2-1～2-3 は複数台あり、端末 3 ではどの負荷分散装置 5-1、5-2 および認証サーバ GW 装置 2-1～2-3 は動作中であり、使用状況（接続数）が少ないと判断できないため、端末 3 は受付サーバ 4 に認証サーバ GW 装置 2-1～2-3 のアドレスを問合せる。受付サーバ 4 では、それぞれの負荷分散装置 5-1、5-2 の生死状態および使用状況（接続数）を認識しているため、動作中で使用状況（接続数）の少ない負荷分散装置 5-1、5-2 のアドレスを求め、端末 3 に負荷分散装置 5-1、5-2 のアドレス IP:3 を返送する。

【0030】端末 3 は認証サーバ GW アドレス問合せで得られたアドレス IP:3 に対して IPsec コネクションの接続要求を行う。IPsec 接続要求（認証）は負荷分散装置 5-1 で受け、負荷分散装置 5-1 では認識している認証サーバ GW 装置 2-1、認証サーバ GW 装置 2-2 の生死状態より動作中の認証サーバ GW 装置に負荷分散することで、認証サーバ GW 装置 2-2 に転送される。認証サーバ GW 装置 2-2 では認証を行い、認証結果が許容であれば、IPsec 接続応答（認証）で応答する。

【0031】このように、端末は、受付サーバに問合せて得られたアドレスに接続することになり、複数の負荷分散装置および認証サーバを意識することなく、認証サーバ群に接続ができる。受付サーバは、負荷分散装置の生死状態を監視しているから、端末は死んでいる負荷分散装置に接続することはない。負荷分散装置は、認証サーバ GW 装置の生死状態を監視しているため、端末は死んでいる認証サーバ GW 装置に接続することはない。受付サーバと認証サーバ GW の間に負荷分散することにより、負荷分散装置にて認証サーバの生死状態を監視するから、受付サーバの監視数が減り、ネットワークへの負荷が低減する。受付サーバは、負荷分散装置に対する使用状況（接続数）を監視しているため、負荷の偏った認証サーバ GW 装置が発生しない。

## 【0032】

【効果の説明】以上説明したように、本発明によれば、複数の認証サービスGW装置の負荷分散を可能とし、併せてダイアルアップ端末からの膨大な数のIPsecコネクション確立を可能とすることができる。

## 【図面の簡単な説明】

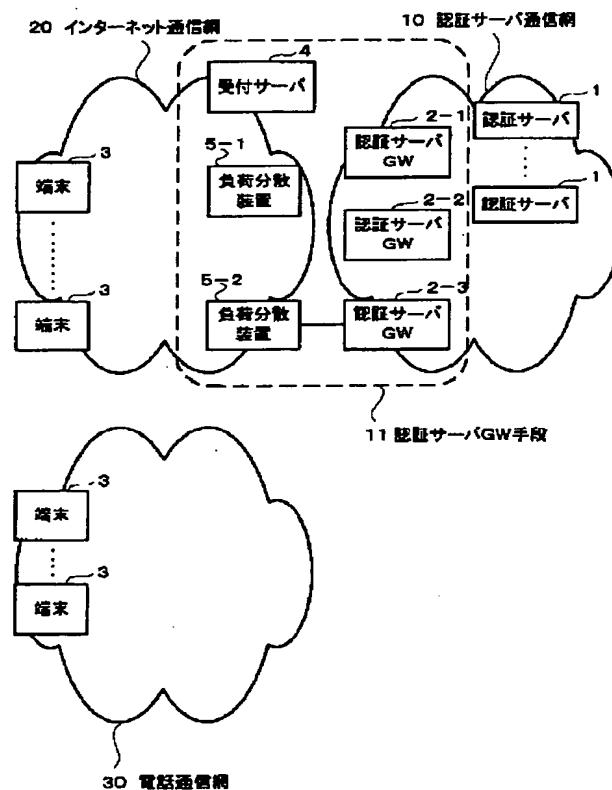
【図1】本発明実施例のインターネット負荷分散中継接続方式の全体構成図。

【図2】本発明実施例のインターネット負荷分散中継接続方式の動作を示すシーケンス図。

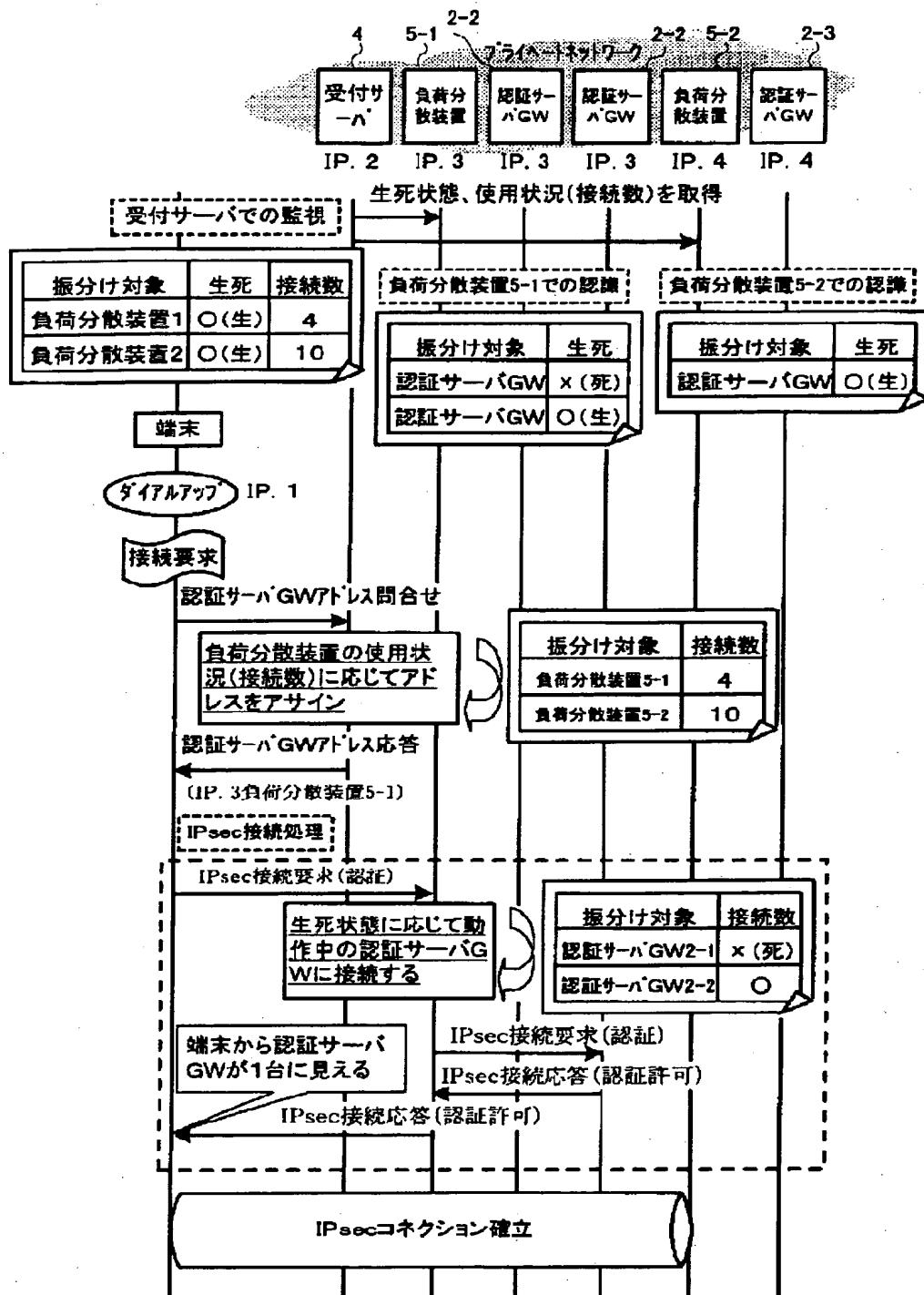
## 【符号の説明】

- 1 認証サーバ
- 2-1～2-3 認証サーバGW装置
- 3 端末
- 4 受付サーバ
- 5-1、5-2 負荷分散装置
- 10 認証サーバ通信網
- 11 認証サーバGW手段
- 20 インターネット通信網
- 10 30 電話通信網

【図1】



【図2】



フロントページの続き

(72) 発明者 井上 拓也

東京都千代田区内幸町一丁目1番6号 エ  
ヌ・ティ・ティ・コミュニケーションズ株  
式会社内

(72) 発明者 溝口 陽一

東京都千代田区内幸町一丁目1番6号 エ  
ヌ・ティ・ティ・コミュニケーションズ株  
式会社内

F ターム(参考) 5B089 GA11 GA31 JB16 KA06 KA07  
KA12 KB04 KC47  
5K051 AA01 BB02 CC01 CC02 FF04  
GG02

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**